

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Rhode Island

United States of America

v.

Himanshu Asri

Defendant(s)

Case No.

1:20-MJ-05195

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February, 2019 in the county of _____ in the
 _____ District of Rhode Island, the defendant(s) violated:

*Code Section**Offense Description*

18 U.S.C. § 1343;
 18 U.S.C. § 1349; and
 18 U.S.C. § 2326.

Wire fraud;
 Conspiracy to commit wire fraud; and
 Telemarketing or email marketing fraud.

This criminal complaint is based on these facts:

See the attached Affidavit of Special Agent, Craig A. Graham, of the Federal Bureau of Investigation ("FBI").

☒ Continued on the attached sheet.

Complainant's signature

Special Agent, Craig A. Graham ~ FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

Jan 13, 2020


Judge's signature

City and state:

Providence, Rhode Island

Patricia A. Sullivan, U.S. Magistrate Judge

Printed name and title

PER 18 U.S.C. 3170

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ INFORMATION ☐ INDICTMENT ☒ COMPLAINTCASE NO. 1:20-mj-05717Matter Sealed: ☐ Juvenile ☐ Other than Juvenile
☐ Pre-Indictment Plea ☐ Superseding ☐ Defendant Added
☐ Indictment ☐ Charges/Counts Added
☐ Information

Name of District Court, and/or Judge/Magistrate Location (City)

UNITED STATES DISTRICT COURT RHODE ISLAND
DISTRICT OF RHODE ISLAND Divisional OfficeName and Office of Person
Furnishing Information on
THIS FORM AARON WEISMAN
☒ U.S. Atty ☐ Other U.S. Agency
Phone No. (401) 709-5000Name of Asst.
U.S. Attorney
(if assigned) Milind M. Shah

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

FBI ~ Craig A. Graham, Special Agent☐ person is awaiting trial in another Federal or State Court
(give name of court)☐ this person/proceeding transferred from another district
per (circle one) FRCrP 20, 21 or 40. Show District☐ this is a reprosecution of charges
previously dismissed which were
dismissed on motion of:☐ U.S. Atty ☐ Defense☐ this prosecution relates to a
pending case involving this same
defendant. (Notice of Related
Case must still be filed with the
Clerk.)☐ prior proceedings or appearance(s)
before U.S. Magistrate Judge
regarding this defendant were
recorded underSHOW
DOCKET NO.MAG. JUDGE
CASE NO.Place of
offense RHODE ISLAND County

USA vs.

Defendant: Himanshu AsriAddress: Delhi
India☐ Interpreter Required Dialect: _____Birth Date 1/20/1987 ☒ Male ☐ Alien
☐ Female (if applicable)

Social Security Number _____

DEFENDANT

Issue: ☒ Warrant ☐ Summons

Location Status:

Arrest Date _____ or Date Transferred to Federal Custody _____

☐ Currently in Federal Custody☐ Currently in State Custody☐ Writ Required☐ Currently on bond☐ Fugitive

Defense Counsel (if any): _____

☐ FPD ☐ CJA ☐ RET'D☐ Appointed on Target Letter☐ This report amends AO 257 previously submitted

OFFENSE CHARGED - U.S.C. CITATION - STATUTORY MAXIMUM PENALTIES - ADDITIONAL INFORMATION OR COMMENTS

Total # of Counts 3

Set	Title & Section/Offense Level (Petty = 1 / Misdemeanor = 3 / Felony = 4)	Description of Offense Charged	Felony/Misd.
	See Attached		<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
		Estimated Trial Days: 5	<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor

**ATTACHMENT TO DEFENDANT INFORMATION RELATIVE TO A CRIMINAL
ACTION - IN U.S. DISTRICT COURT**

DEFENDANT: Himanshu Asri

COUNT I: 18 U.S.C. § 1343: Wire Fraud - Felony.

MAXIMUM PENALTIES: Imprisonment: 20 years; Supervised release: 3 years; Fine: \$250,000; and Special assessment: \$100.

COUNT II: 18 U.S.C. § 1349: Conspiracy to commit the aforementioned frauds - Felony.

MAXIMUM PENALTIES: Imprisonment: 30 years; Supervised release: 5 years; Fine: \$250,000; and Special assessment: \$100.

COUNT III: 18 U.S.C. § 2326: Telemarketing or email marketing fraud - Felony.

MAXIMUM PENALTIES: Imprisonment: 5 years; Supervised release: 3 years; Fine: \$250,000; and Special assessment: \$100.

AFFIDAVIT OF FBI SPECIAL AGENT CRAIG A. GRAHAM

I. Introduction

I, Craig A. Graham, having been duly sworn, state as follows:

1. Since 2010, I have been a special agent with the Federal Bureau of Investigation ("FBI"). Early in my career, I focused on counterintelligence investigation. Starting in 2015, my responsibilities expanded to include the investigation of wire fraud, mail fraud, and other white collar crimes. Since July 2018, when I was assigned to the FBI's Providence Resident Agency, I have focused primarily on white collar investigation. I have experience in the investigation of telemarketing fraud, and through that work have gained a familiarity with computer or smartphone based communication applications such as WhatsApp, Snapchat, and Skype. I also have experience in the examination of electronic devices, including computers and cellular telephones or smartphones, for evidence, including electronic mail, toll records, text messages, geolocation information, photographic records, and records associated with WhatsApp, Snapchat, and Skype.

2. I submit this affidavit in support of a criminal complaint and arrest warrant charging Himanshu Asri (born January 1987) ("Asri"), a male who resides in India, with the following offenses:

- (i) wire fraud, in violation of 18 U.S.C. § 1343,
- (ii) conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, and
- (iii) telemarketing or email marketing fraud, in violation of 18 U.S.C. §§ 2326.

3. The information in this affidavit comes from my personal observations and investigation, my training and experience, other law enforcement agents, a cooperating source of information, and other sources as specified in the body of this affidavit. This affidavit is intended to show that there is sufficient cause for the requested warrant and does not set forth all of my knowledge about this matter or investigation.

4. Based on my investigation, I believe that there is probable cause to believe the following:

a. Asri and coconspirators schemed (i) to deceive victims into believing that their computers had been or were being attacked by malware and (ii) to use that deception to obtain money from victims by purporting to sell computer protection services to the victims;

b. as part of the scheme, both to mislead victims and to aid in the extraction of money from victims, Asri's coconspirators falsely represented themselves to be affiliated with known computer software and computer services corporations, such as Microsoft; and

c. Asri and his coconspirators executed or attempted to execute this scheme on at least 325 occasions.

II. Investigation

Summary

5. The investigation, which is described below, indicates that there is probable cause to believe that from January 2019 to March 2019, Asri obtained 325 telephone calls from U.S. callers who had been misled into believing that malware attacks had been detected on their computers, and then Asri had those calls routed to call centers where operators offered purported computer protection services to the callers to extract or attempted to extract money from the callers. The investigation, as described below, was based (i) on information provided to the FBI by one of Asri's coconspirators, (ii) historical text communications between the cooperating coconspirator and Asri or from a group that included Asri, (iii) records and call recordings obtained from a call routing platform used by that coconspirator, and (iv) interviews of some of the callers.

6. FBI agents listen to eight of the calls and spoke to three of the callers. The information provided by those call reviews and callers combined with the information from the cooperating coconspirator and records associated with the call routing platform he used lends probable cause to believe that all 325 calls were obtained by Asri for the purpose of defrauding the callers. From the eight call recordings, there is probable cause to believe that there was an

attempt to extract at least \$499 from each of the 325 callers, yielding an overall intended fraud loss in excess of \$150,000.

Initial Information Provided by the Cooperator

7. In May 2019, the FBI arrested a male in the United States on charges that included conspiracy to defraud and multiple instances of wire fraud and bank fraud. The male shortly after his arrest began cooperating with the FBI in the hope of receiving leniency in the disposition of the pending charges. The male is hereinafter referred to as the "Cooperator."

8. The Cooperator, an Indian citizen and resident, has not previously been convicted of any crimes in the United States. The FBI is not aware of whether the Cooperator has ever been convicted of crimes in India, but the Cooperator reports that he has never been jailed in India.

9. In May 2019, after his arrest, the Cooperator told me that an acquaintance, Asri, was involved in telemarketing scams that defrauded people residing in the United States.

10. The Cooperator described himself and Asri as brokers. They bought telephone call traffic, specifically calls placed by people who, based on advertising that they had seen on their computers, believed that their computers had been or were being attacked by malware. The Cooperator explained that such advertising was not based on any information indicating that the callers' computers had malware problems and that the advertising was often targeted toward those likely to lack computer or software expertise.

11. The Cooperator explained that he had sold such call traffic to Asri and had per Asri's instructions directed the call traffic to call center operators who solicited the callers to purchase purported computer assistance services. The Cooperator also said that Asri was affiliated with a particular call center.

12. The Cooperator described the role of "publishers" in the telemarketing fraud industry. He explained that publishers created various forms of online advertising, including

pop-up ads,¹ designed to mislead viewers into believing that malicious software or malware was attacking their computers. For example, the Cooperator suggested that a publisher could place ads on Facebook offering travel agent services for retirees interested in cruise vacations. A viewer who clicked on the ads would be directed to a page that would state that the viewer's computer had been infected by a virus or was being attacked by malware and advise the viewer to call a particular telephone number.

13. The Cooperator explained that brokers could purchase from a publisher the calls generated by such advertising. Using call routing technologies, the publisher would route incoming calls to the broker. The broker in turn could sell the calls by re-routing them directly to call centers or to other brokers who ultimately had the calls routed to call centers.

14. The Cooperator explained that call centers, specifically those involved in telemarketing fraud, were facilities designed to accept incoming calls and extract money from the callers. Typically, call centers were comprised of multiple operators, each of whom would be familiar with the sort of advertising that had been seen by the callers. The operators would accept the calls generated by the publishers' advertising and seek to extract money from the callers by purporting to provide computer protection services.

15. The Cooperator said that prior to his arrest by the FBI and prior to becoming a source of information for the FBI, he had routed call traffic to Asri knowing that the callers would be defrauded or that there would be an attempt to defraud the callers; that call traffic routed by the Cooperator to Asri included many calls from U.S. telephone numbers; that Asri was involved in the operation of a call center in Subhash Nagar in New Delhi, India, and that call center had approximately 10 employees; and that in selling Asri call traffic, the Cooperator utilized a third party's call-tracking and routing software platform ("CRS").

¹ The Cooperator explained, and I know from my training and experience, that pop-up ads are a particular form of online advertising. While one is browsing internet sites, a separate browser window pops up, and that new window must be closed or disabled in order to continue browsing activities.

Identification of Asri and His Communication Accounts

16. The Cooperator identified a particular WhatsApp account² as belonging to Asri. The telephone number associated with the account was 919811873895, an Indian telephone number.³

17. Documents obtained from the Department of State show that that same telephone number, 919811873895, was listed as the home telephone number for Asri on his United States Visa application. The Visa application included a photograph of Asri, which the Cooperator identified as Asri. I, therefore, believe that there is probable cause to believe that the aforementioned WhatsApp account and telephone number belong to Asri. A copy of Asri's Visa application photograph is attached as Exhibit 1.

18. The Cooperator identified a particular Skype account⁴ as belonging to Asri. That account lists the vanity name, a user selected name, "Himanshu Asri" and an account name of "himanshuasri." This Skype account also lists the account holder's birth day as "1/20." Asri's Visa application listed a date of birth of January 20, 1987. I therefore believe that there is probable cause to believe that the aforementioned Skype account belongs to Asri.

19. The Cooperator identified Asri's Facebook account, an online social media platform which allows users to create a profile page, upload photographs, share texts, and share their current location. Asri's Facebook account included photographs of the purported account

² WhatsApp is a communications applications for mobile devices and desktop computers that allows users to send and receive text and voice messages, make and receive voice and video calls, and share images, documents, user location, and other media. All users of the application must have an account or access to an account. In the account creation process, users provide a cellular mobile number. WhatsApp is owned by Facebook, Inc.

³ A picture of two older people is associated with the account, but neither appears to be the account holder. A caption associated with the picture indicates that the persons photographed have passed away. The caption states "No One Can fill this Void. Luv u till eternity[.]"

⁴ Skype is a communications application for mobile devices and desktop computers that allows users to send and receive text and voice messages, make and receive voice and video calls, and share images and other media. All users of the application must have an account or access to an account. Skype is owned by Microsoft Corporation.

holder. The Cooperator identified the profile page as belonging to Asri and identified Asri as the person in the page's pictures. The person in the pictures is also visually similar to the individual in Asri's Visa application photograph. Attached as Exhibit 2 is a screen shot of Asri's Facebook profile page.

20. As described below, Asri arrived in the United States on December 27, 2019 and told customs officials that he owned a furniture showroom in India and had rental incomes. Upon arrival, Asri was photographed by customs officials, I reviewed those photographs, and his appearance is consistent with that of the person in Exhibit 1 and Exhibit 2. The customs photograph of Asri is attached as Exhibit 3.

2018 and Early 2019 Text Message Concerning Sale of Call Traffic to Asri

21. The Cooperator voluntarily provided access to his CRS account, and from records in that account, I was able to isolate calls that had been directed to Asri. Those calls are further categorized in the records by "Affiliate" name, specifically the party directing the call traffic to the Cooperator's account, and by "Target" name, specifically the party that the call traffic is directed to. The Affiliate and Target names are assigned by the account user, in this case the Cooperator, and this feature on the CRS platform allows the user to track the call volume generated by those directing call traffic to the user's account and to track the call volume directed to targets. The Cooperator advised that calls routed to Asri were identified in the CRS records by the Target name "DeltaHimanshu."⁵

22. According to records from the Cooperator's CRS account, from January 2019 to March 2019, the Cooperator sold approximately 325 calls provided by others (who the Cooperator characterizes as publishers) to "DeltaHimanshu9127," Asri according to the Cooperator. The records also indicate that callers or victims included one from a telephone

⁵ From the time of arrest to the present, the Cooperator has assisted FBI agents in reviewing his CRS account records. During such reviews, the Cooperator accompanied by one or more FBI agents and no records were altered.

number with a Rhode Island area code. 324 of the calls were from callers with U.S. area codes, and one of the calls was from a caller with a Canadian area code.

23. The Cooperator in July 2019, on reviewing the CRS account records, identified these 325 calls as the calls he sold to Asri for the purpose of having the callers defrauded.

24. The Cooperator, after he was arrested in May 2019, allowed investigators to extract electronic records from his cellular telephone. The extraction revealed WhatsApp and Skype text communications between the Cooperator's WhatsApp and Skype accounts and Asri's WhatsApp and Skype accounts. In the text messages set forth below, which fall within the June 2018 to March 2019 time period, Asri, the Cooperator, and others discussed Asri purchasing call traffic from the Cooperator.

25. In June 2018, the Cooperator, the Cooperator's office manager ("Manager"), and Asri created a Skype group. The Cooperator told FBI agents that the group was created to facilitate text conversation between the three about Asri's purchasing call traffic from the Cooperator. On June 20, 2018, Asri sent a screen shot to the group in which a fund transfer to the Cooperator is displayed. Also visible in the screen shot is a Skype application which displays the Skype user name "himanshuasri."

26. In the following Skype text exchange, which was dated July 10, 2018, Asri requested access to the Cooperator's previous CRS account and Asri provided his email account. I know from having developed a familiarity with the CRS platform that provision of email account is a necessary step for a Target to obtain access to another's CRS account. The email provided is identical to the email Asri listed on his Visa application. In the exchange, Asri also made several requests to the Cooperator's Manager seeking to know the total number of calls that had been sent to Asri from the Cooperator's previous CRS account. The time stamp associated with each text is included below; based on the text messages, it appears that as time passed, Asri received more and more calls, and then at a certain point, Asri indicated that the work day was done and requested that the call routing be paused. Asri signaled that no additional calls should be sent by texting "eod" meaning "end of day." Times are listed how

they appeared on the Cooperator's phone and are in India Standard Time, which is 9.5 hours ahead of Eastern Daylight Time in the U.S.

Timestamp-Date	From	Body
07/10/2018; 1:05am	Asri	Can we please have access to [Cooperator's previous CRS] it will be really appreciated
07/10/2018; 1:05am	Manager	he is in meeting will do it
07/10/2018; 1:05am	Asri	himanshuasri@gmail.com thanks meanwhile can u please tell how many calls so far
07/10/2018; 1:09am	Manager	15
07/10/2018; 1:09am	Asri	ok
07/10/2018; 2:24am	Asri	how many calls?
07/10/2018; 2:24am	Manager	28
07/10/2018; 2:39am	Asri	ho many?
07/10/2018; 2:39am	Manager	29
07/10/2018; 3:32am	Asri	total calls?
07/10/2018; 3:32am	Manager	35
07/10/2018; 3:33am	Asri	eod pause plz
07/10/2018; 3:33am	Manager	ok

27. In the following Skype text exchange, dated January 10 and 11 in 2019, the Cooperator's Manager advertised "high quality" calls for sale with a "guaranteed RPC over \$70-100" meaning, as explained by the Cooperator, that the buyer is guaranteed to make an average "return per call" of \$70 to \$100 dollars. The Cooperator's Manager also advertised that

“any cc doable,” meaning, as explained by the Cooperator, that a volume of calls was for sale for any “cc” meaning concurrent calls, a measurement of how many calls a call center can handle at one time. The calls were on sale for \$17 per call.

Timestamp-Date	From	Body
01/10/2019	Manager	High quality calls with guaranteed RPC over \$70-100 , any cc doable .. if you don't get the RPC then dont pay
01/10/2019	Asri	Rate
01/10/2019	Manager	\$17
01/10/2019	Asri	Calls are worth ?
01/10/2019	Cooperator	Yo
01/10/2019	Asri	Okay Will resume Then Later
01/10/2019	Cooperator	Done
01/10/2019	Asri	But ask him no reminder for payment I ll make payment on own
01/10/2019	Manager	Sir prepay
01/10/2019	Cooperator	Sir cc Now [Manager] No pre pay here 500 calls advance
01/10/2019	Asri	Thanks [Cooperator] Sir
01/10/2019	Manager	Cc?
01/10/2019	Asri	Around 10

28. Later the same day, Asri provided by Skype text a toll free number, 855-855-9127, to the Cooperator for calls to be routed to. And on January 11, 2019, the Cooperator's manager sent a message to the group stating "7 calls yesterday" and provided the date, time, duration, and originating telephone number of each call. One of the calls had an originating telephone number from area code 330.

First of Eight Calls Reviewed and Contact with Caller, LD

29. In the Cooperator's CRS account, FBI agents located the call that originated from the aforementioned 330 area code. Based on review of that call, interviewing the caller, a review of Microsoft policy, and the unusual manner in which payment was sought, there is probable cause to believe that there was an effort to defraud the caller. Based on the communications described in paragraph above, there is probable cause to believe that that effort to defraud involved Asri.

30. A review of the Cooperator's CRS account showed that on January 10, 2019, a call from the aforementioned telephone number from area code 330 was directed to Asri by the Cooperator. FBI agents listened to the call, a voice recording of which is preserved by the CRS platform, and the following is a summary of the call:

- The Operator answered the call and told the caller they were calling "Technical Support."
- The caller told the Operator that Microsoft says she is locked out of her computer and to call Microsoft.
- The Operator told the caller there was a third party attack on her computer and a Trojan horse had crashed her network security and gotten into her IP address.
- The Operator directed the caller to a website that would allow the Operator to remotely connect to the caller's computer.
- The Operator told the caller that she would check with a "Microsoft Expert" and see what the caller needed to protect against the attack.
- The Operator told the caller that the matter would be assigned to a Microsoft Level 12 Technician who would remove the third party infection, stop the illegal access to her computer, block the hacking and fake software and repair her IP address and firewall.

- The Operator told the caller that there were three plans: a onetime fix for \$199, a one year security plan for \$299, and a lifetime security plan for \$499.
- The caller provided her name, email address, phone number, and address.
- The Operator provided the caller with two customer service numbers: 855-704-1391 and 855-855-9127.⁶
- The caller was directed to pay by check. The Operator told the caller to make the check payable to Technical Support (Microsoft) in the amount of \$499.
- The Operator then activated the camera on the caller's computer and took a photograph of the check.

31. Using the caller's telephone number and information provided during the call, FBI agents identified and located the caller, hereafter referred to as LB, at her home in Ohio. LB, who is approximately 60 years old, provided agents with personal identifiers that matched the information obtained during the recorded phone call. LB also relayed the following to agents:

- While visiting her banks online web page she received a pop up message stating she had been "locked out" of her computer. The pop up message listed a phone number to contact for assistance.
- LB dialed the number and the call was answered by a foreign sounding individual who told LB that her computer had likely been hacked or infected with a virus. For a fee the individual could remotely access her computer and remove the virus.
- The individual downloaded an application called "Any Desk" on to LB's computer and took remote access of her computer.
- After a few minutes, the individual advised her that the virus had been removed and payment was due.
- LB wrote a check made payable to "Technical Support/Microsoft," and held the check up to the computer's camera for the individual to take a picture. LB believed the check was for approximately \$499.00. The individual also confirmed LB's bank account number and routing number.
- The individual asked if LB's computer was unlocked, and then ended the phone call.
- Shortly after, LB started to believe that call was a scam because of the high price she was told to pay. LB went to her bank and closed the account she wrote the check from.

⁶ Telephone number 855-704-1391 appeared in ten complaints received by the FBI related to two technical support websites registered currently or historically to Asri. Telephone number 855-855-9127 is currently displayed on the website for Technical Support Today, www.technicalsupporttoday.com, which is registered to Asri.

- Within a few days, LB received a message from the individual on her cellular phone to call the individual back.

32. Microsoft policy, as set forth on its publically accessible website, www.microsoft.com, in the section entitled "Protect yourself from tech support scams," specifies that "Microsoft error and warning messages never include a telephone number."

Text Message from Asri Concerning Payment to Cooperator

33. On February 1, 2019, in Skype text communications, the Cooperator asks Asri to wire money to a US bank account as payment for the calls previously routed to Asri. In a subsequent message, Asri writes that \$2,000 has been transferred to the Cooperator's account.

Request from Asri for More Call Traffic

34. In the following Skype text exchange, dated February 4 and 5 in 2019, Asri requests "2cc" or 2 concurrent calls worth of call traffic and discusses the number of calls being directed to him. The Cooperator's Manager again sends a summary of the calls sent the previous day, which includes the date, time, duration, and originating telephone number of the calls sold to Asri. One of the calls had an originating telephone number from area code 713.

Timestamp-Date	From	Body
02/04/2019	Asri	Start with 2 cc Done? ? ? ? ?
02/04/2019	Manager	ok doing
02/05/2019	Asri	not getting calls
02/05/2019	Manager	1 live
02/05/2019	Asri	k make it 2 cc
02/05/2019	Manager	Ok

02/05/2019	Asri	2 avail ?
02/05/2019	Manager	trying to increase sir plz wait
02/05/2019	Asri	Hi Eod ho gaya kya bhai [Brother did EOD happen] ⁷ ??
02/05/2019	Manager	Nhi [No]
02/05/2019	Asri	Phir calls do [Then give me calls] Yaar [Friend] eod pause plz
02/05/2019	Cooperator	It's auto
02/05/2019	Manager	6 calls yesterday
02/05/2019	Manager	[Provides a list of the six calls received on 2/4/2019. The list provides the date, time, duration of the call and the phone number the call originated from. This list included a call that originated from 713-XXX-XXXX]

Second of Eight Calls Reviewed and Contact with Caller, GP

35. In the Cooperator's CRS account, FBI agents located the call that originated from the aforementioned 713 area code. Based on review of that call, interviewing the caller, a review of Microsoft policy as described in paragraph 32, and the representation of association with Microsoft and later amendment at time of billing, there is probable cause to believe that there was an effort to defraud the caller. Based on the communications described in paragraph above, there is probable cause to believe that that effort to defraud involved Asri.

⁷ The Hindi portions of text communications have been translated by a linguist fluent in Hindi and English.

36. A review of the Cooperator's CRS account showed that on February 4, 2019, a call from the aforementioned telephone number from area code 713 was directed to Asri by the Cooperator. The following is a summary of that call:

- The Operator answered the call and told the caller they were calling "Technical Support for Microsoft."
- The Operator directed the caller to a website that would allow the Operator to remotely connect to the caller's computer.
- The Operator told the caller that his system registry had been corrupted by foreign entities and the caller's anti-virus software did not protect against a hacking attack or Trojan. The operator explained that a Trojan was a third party hacking attack.
- The Operator said that he would check with a Microsoft Expert to see how the computer could be fixed, and there was a onetime fee associated with the fix, which would be a minimum of \$99.
- The Operator told the caller that he would assign a Level 12 Technician. The Level 12 Technician would remove the Trojan, put a stop on all illegal access, and put a block on all the hacking and fake software.
- The Operator told the caller that there were three plans: a onetime fix for \$199, a one year security plan for \$299, and a lifetime security plan for \$499.
- The caller said he would take the One Year Security Plan for \$299.
- The caller provided his name, email address, phone number, and address.
- The Operator provides the caller with a 24/7 toll-free number for the Microsoft Technicians. The numbers provided were 855-704-1391 and 855-855-9127.⁸
- The caller told the Operator he would pay via credit card and provided the name on the card, the credit card number, expiration date, and three digit code on the back.
- The Operator told the caller that his computer was not receiving updates and that was why his computer had a hacking attack.
- The Operator also told the caller that the software warranty on his computer had expired and asked the caller if he wanted the Technician to update the software warranty on his computer for a separate charge.
- The Operator asked if the caller is over 60. The Caller told the Operator he was not, but that he was a military veteran.

⁸ See *supra* note 6.

- The Operator asked if he wanted to purchase the Microsoft Software Warranty plan. The plans are 1 year for \$150, a three year plan at \$50 per year or a five year at \$70 per year.
- The caller said he would will take the 5 year which was \$70 per year for \$350 total. The \$350 would cover up to five computers.
- The Operator confirmed that the caller was purchasing a One Year Security Plan and a five year Software Warranty.
- The Operator told the caller the charge would appear under the name Technical Support only, the company that manufactures all the security, not Microsoft.
- The Operator told the caller that American Express declined the charge and directed the caller to check his phone to see if there was a text message to verify the charge which would be \$641 USD or 46,000 Indian Rupees.
- The caller said he had a text from American Express and saw the charge for 46000 Indian Rupees. The Operator stated that their billing department was located in India.
- The Operator said he received confirmation from the billing team that the charge had been approved by American Express because they saw the charge was from a Microsoft Technician.

37. Using the phone number and information provided during the call, FBI agents identified and located GP at his home in Texas. GP, who is approximately 50 years old, provided agents with personal identifiers that matched the information obtained during the recorded phone call. GP also relayed the following to agents:

- On or about February 7, 2019, while GP was working on his computer an error message from Microsoft appeared on his computer screen which indicated that something was wrong with his computer and he needed to call a provided customer service number.
- GP called the telephone number and spoke to David at extension 422 who had an Indian accent.
- David directed GP to a website called "Any Desk" and had GP provide the code on the screen. Once GP provided the code, he saw the cursor move all over the screen.
- A short time later, David LNU told GP that his computer had 100 viruses and it would cost \$645.25 to repair his computer.
- GP asked if David would accept a credit card and David stated he would. GP then made payment to David.
- GP noticed that David put an Any Desk shortcut and "Technical Support" text document on his computer.

- GP showed agents a Subscription and Security Protection agreement for his computer. The agreement listed two technical support numbers, 855-704-1391 and 855-855-9127, and a case ID number.
- On June 4, 2019, GP's computer was slowing down and he called the technical support phone number on his computer.
- Again an individual with an Indian accent answered and asked GP for his case ID number. GP was then directed to the Any Desk icon on his computer in order to again provide remote access to his computer.
- The individual told PG that his computer had viruses and it would cost \$990.97 to repair his computer and provide him with the "life time plan." GP again paid the higher price with his credit card.
- GP provided Agents with a copy of his credit card statement that showed on February 8, 2019, he paid "Technical Support Today Computers and Equipment" in New Delhi 46,000 Indian Rupees, which is \$645.25.

Third of Eight Calls Reviewed and Contact with Caller, DH

38. On February 14, 2019, the Cooperator's Manager sent via Skype text to the Cooperator and Asri a summary of the 13 calls sent the previous day to Asri, which included the date, time, duration, and originating telephone number of the calls sold to Asri. One of the calls had an originating telephone number from area code 320.

39. In the Cooperator's CRS account, FBI agents located the call that originated from the aforementioned 320 area code. Based on review of that call, interviewing the caller, a review of Microsoft policy as described in paragraph 32, the representation of association with Microsoft but differing party to whom payment was directed, and the unusual manner in which payment was sought, there is probable cause to believe that there was an effort to defraud the caller. Based on the communications described in the paragraph above, there is probable cause to believe that that effort to defraud involved Asri.

40. A review of the Cooperator's CRS account showed that on February 13, 2019, a call from the aforementioned telephone number from area code 320 was directed to Asri by the Cooperator. The following is a summary of that call:

- The Operator answered the call and told the caller they were calling "Microsoft Support."
- The caller told the Operator that he got a message on his computer from Microsoft that someone had hacked into his computer.

- The Operator then directed the caller to a website that would allow the Operator to remotely connect to the caller's computer.
- Once the operator was remotely connected, he told the caller there was a third-party spy "Clampi" on the caller's computer that has crashed the caller's network security and gotten into his IP address.
- The Operator also told the caller his anti-virus software did not protect against a hacking attack or Trojan and that was why the alert was appearing on his computer screen.
- The Operator then tells the caller there are three plans: a onetime fix for \$199, a one year security plan for \$299 and a lifetime security plan for \$499.
- The caller provided his name, email address, phone number, and address. The caller also stated that he was a School Bus driver and he is over 60 years old.
- The Operator said that because he was a Senior Citizen, the lifetime security plan would only cost \$399.
- The Operator then provided the caller with two customer service numbers, 855-704-1391 and 855-855-9127,⁹ and directed the caller to pay by check. The Operator told the caller to make the check payable to Technical Support (Microsoft) in the amount of \$399.
- The Operator directs the Caller to put the check on the scanner in order for the Operator to take a copy of the check.

41. Using the phone number and information provided during the call, FBI agents located DH at his home in Minnesota. DH, who is approximately 63 years old, provided agents with personal identifiers that matched the information obtained during the recorded phone call. DH also relayed the following to agents:

- On or about February 13, 2019, DH was using his computer when a "pop up" appeared on his screen indicating he should call a provided telephone number right away or he would lose information on his computer.
- DH called the number and spoke with "David at extension 422" who told DH that he worked for Microsoft.
- David told DH that he could fix his computer, but it would cost money to do so and offered a "2 year unlimited technical support warranty" in exchange for the fee.
- David told DH that he would need to gain remote access to DH's computer in order to fix the error.
- David first asked DH for a credit card for payment, but because DH did not have a credit card, he wrote out a check for \$399.95. DH made the check out to

⁹ See *supra* note 6.

"Technical Support/ Microsoft" and David told DH to write "Lifetime Security" on the memo line. DH was also instructed to scan the check into his computer.

- After the check had been scanned, DH received an email receipt showing that he paid \$399.95 for "2 year unlimited technical support warranty."
- The email came from an electronic check processor and indicated that DH's payment went to "Best Tech 247."
- After speaking with his sister, DH believed he was a victim of a scam and closed the account from which he had written the check.
- Shortly after DH closed the account he received a telephone call from David asking for a new check because the first one would not go through for payment. DH told David that he would not write another check.

Fourth and Fifth of Eight Calls Reviewed

42. A review of the Cooperator's Skype communications between Asri and the Cooperator's manager indicated that 30 calls were sold to Asri around February 23, 2019, however the Cooperator's manager shared only the total number of calls with Asri and did not share the call details. Accessing the Cooperator's CRS Account, FBI agents reviewed two of those 30 calls.

43. In the CRS account records, the first of those 30 calls, which was dated February 23, 2019, was routed to Asri, and originated from an identified telephone number with area code 412. Based on review of that call, the representation of association with Apple, and the unusual manner in which payment was sought, there is probable cause to believe that there was an effort to defraud the caller. The following is a summary of the call:

44. One of the calls within the Cooperator's CRS Account, dated February 23, 2019, was routed to Asri and originated from an identified telephone number with the area code 412. The following is a summary of that call:

- The Operator answered the call and told the caller she contacted "Apple Support."
- The Caller stated she received a Virus Alert on her Apple computer.
- The Operator directed the caller to a website that would allow the Operator to remotely connect to the caller's computer.
- The Operator then told the caller that her computer had been hacked and that to fix the security he will charge her for 15 applications that will block the hackers.

- The Operator tells the caller that the 15 applications, \$40 each, will cost a total of \$600.
- The Operator asks the caller to provide her name, phone number, address and email address.
- The caller stated she was poor and would like to pay with a credit card, rather than a check because she had only \$200 in her checking account.
- The Operator told the caller she could pay \$199.99 via check, payable to "Technical Support (Apple)," and pay \$299 on her credit card, which will be billed by Technical Services.
- The Operator told the caller to put the check on the copier/ printer so the Operator can scan a copy of the check and the caller provided the Operator with her credit card number, expiration date and three digit number on the back of her credit card.
- The caller then stated that she could see that her credit card had been charged.

45. A review of Apple's support materials, as set forth on its publically accessible website, www.apple.com, makes plain that telephone numbers that appear in pop-up error messages should not be called. In the Apple support section entitled "Avoid phishing emails, fake 'virus' alerts, phony support calls, and other scams," Apple advises that computer users who see pop-up ads specifying a telephone number to call should not call the number:

"When you browse the web, you might see a pop-up ad or a page warning you about a problem with your device. It might even look like the alert is coming from macOS or iOS. It isn't. These alerts are pop-ups, designed to trick you into calling a phony support number or buying an app that claims to fix the issue. Don't call the number. Simply navigate away from that page, or close the window or tab, and continue browsing."

46. In the CRS account records, the second of those 30 calls was also dated February 23, 2019, was routed to Asri, and originated from an identified telephone number with area code 215. Based on review of that call and the Microsoft policy described in paragraph 32, there is probable cause to believe that there was an effort to defraud the caller. The following is a summary of the call:

- The Operator answered the call and told the caller they were calling "Technical Support" at Microsoft.
- The Caller stated he received a virus alert from Microsoft.

- The Operator told the Caller that it was not a virus and instead a hacking attack on the Caller's IP address.
- The Operator directed the Caller to a website that would allow the Operator to remotely connect to the Caller's computer.
- The Operator told the caller that to fix the problem she would need to remove the hackers from the computer, repair the damage caused by the hackers, and then install a six way security block to protect the computer, printer, router, data and personal identifiers.
- The Operator told the caller that Microsoft does not charge to fix the computer, the only charge is to fix the IP address.
- The Operator told the Caller that Microsoft has three plans: A onetime fix will cost \$199, a one year plan will cost \$299, and a lifetime plan will cost \$499.99.
- The Caller told the Operator she is a Senior Citizen, 88 years old, and living on social security.
- The Operator told the Caller that for Senior Citizen's there are two plans: a onetime fix for \$99 and a lifetime plan for \$199.
- The Caller said they could only pay \$99, and provided their credit card number, expiration date, and three digit code on the back of the credit card.

Six, Seventh, and Eighth of Eight Calls Reviewed

47. A review of the Skype text communications between Asri and the Cooperator's manager, all of which were copied to the Cooperator, indicated that 22 calls were sold to Asri around February 25, 2019, however the Cooperator's manager shared only the total number of calls with Asri and did not share the call details. Accessing the Cooperator's CRS Account, FBI agents reviewed a sample of those calls.

48. One call within the Cooperator's CRS account, dated February 25, 2019, was routed to Asri and originated from an identified telephone number with the area code 386. Based on review of that call and the Microsoft policy described in paragraph 32, there is probable cause to believe that there was an effort to defraud the caller. The following is a summary of the call:

- The Operated answered the call and told the caller he contacted "Microsoft Support"
- The caller stated she had a pop-up on her computer which was a message from Microsoft's Virus Support.

- The Operator directed the caller to a website that allowed the Operator to remotely connect to the caller's computer.
- The Operator then told the caller that her IP address had been blocked and that even if she purchases a new computer the threats would come back.
- The Operator told the caller that he could remove the hackers from foreign locations on her computer, remove all damages on her computer, repair the applications and drivers on her computer, and fix her network, computer and devices.
- The Operator told the caller that Microsoft had three plans: a onetime fix will cost \$199, a one year plan will cost \$299, and a lifetime plan will cost \$399.99.
- Once the caller picks a plan, the Operator will assign a technician.
- The caller stated that she is 74 years old and does not have the money to pay to fix her computer.
- The Operator said that because she was a senior he will give her one year of service for \$199.
- The Operator asked for the caller's name, address, and email address.
- The Operator also asked for the Caller's credit card number, expiration date, and three digit code on the back of her credit card.
- The Operator told the caller that the transaction for \$199.99 had been approved.

49. A second call within the Cooperator's CRS account, dated February 25, 2019, was routed to Asri and originated from an identified telephone number with the area code 305. Based on review of that call and the Microsoft policy described in paragraph 32, there is probable cause to believe that there was an effort to defraud the caller. The following is a summary of that call:

- The Operator answered the call and told the caller he was calling "Microsoft Support."
- The caller told the Operator that he had received a warning from Microsoft.
- The Operator directed the caller to a website that would allow the Operator to remotely connect to the caller's computer.
- The Operator told the caller that a Trojan "Clampi" was found on his computer and described the "Clampi" as a third party software that gets into the system through his IP address.
- The Operator told the caller the he needed to check with a Microsoft Expert to determine what type of security is needed to fix the problem.

- The Operator then said he needed a Microsoft Server Level 12 Technician to repair his computer to remove the third party programming, stop illegal access, block hacking and fake software, and repair complete firewall and IP address.
- The Operator told the caller there were three plans: a onetime fix for \$199, a one year security plan for \$299, and a lifetime security plan for \$499.
- The caller provided his name, phone number, email address and address.
- The caller said he would purchase the one year security plan for \$299.
- The caller provided his credit card number, expiration date and three digit code on the back.
- The Operator told the caller that he may get a call from his credit card company to verify the transaction and the caller should say that he used the credit card.
- The Operator tells the caller that the credit card transaction was approved.

50. A third call within the Cooperator's CRS account, dated February 25, 2019, was routed to Asri and originated from an identified telephone number with the area code 401. Based on review of that call and the Microsoft policy described in paragraph 32, there is probable cause to believe that there was an effort to defraud the caller. The following is a summary of that call:

- The Operator answered the call and told the caller he contacted "Microsoft Support"
- The caller stated a screen came up on his computer saying there was a Microsoft virus alert and to call this number.
- The Operator directed the caller to a website that would allow the Operator to remotely connect to the caller's computer.
- The Operator told the caller there was a third party hacking attack and a Trojan Clampi on his computer which caused the alert.
- The Operator told the caller that his network security had been compromised and that buying a new computer would not fix the problem because his IP address had been corrupted.
- The Operator stated that he would check with a Microsoft Expert to see how the Caller's computer can be fixed.
- The Operator then told the caller there would be a onetime fee to fix his computer that would cost a minimum of \$70.00.
- The Caller stated that he did not have the money, and asked if he could call back.
- The Operator told the caller he could call back, but could not use his computer until it was fixed.

Websites Registered to Asri and associated Internet Complaints

51. Additional information links Asri to the calls routed to the operators.

52. Using a publically available search tool, the FBI obtained domain registration information for "besttech247.com" and found that Asri was listed as the registrant for the website. As noted above, caller DH's payment check went to or was routed to Best Tech 247.

53. The FBI also obtained domain registration information for "technicalsupporttoday.com," "technicalsupporttoday.net," and "technicalsupporttoday.org" and found that Asri was also listed as the current or historical Registrant for those websites.

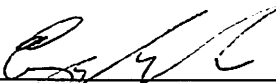
54. Since 2000, the FBI has operated the Internet Crime Complaint Center ("IC3") to provide the public with a method to submit information to the FBI concerning suspected Internet-facilitated criminal activity. The FBI maintains a searchable record of the complaints submitted to IC3.

55. A search of IC3 complaints related to "Technical Support Today" resulted in 23 complaints resulting in losses of over \$50,000. A search of complaints related to "Best Tech 247" resulted in 15 complaints resulting in losses and over \$14,000.

56. These complaints range from 2012 to 2019. A review of these complaints found multiple similarities between the complaint narratives and the aforementioned call recordings which were reviewed above. Some of those similarities included the use of the name David, requesting remote access from the victim, payment methods, and purported affiliation with Microsoft.

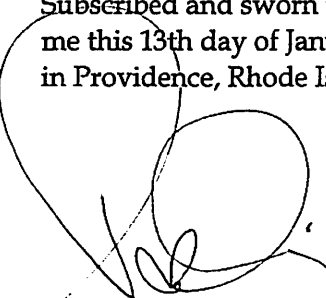
III. Conclusion

57. Based on the above, I believe that there is probable cause to believe that Asri committed the offenses specified in paragraph 2 above.



Special Agent Craig A. Graham
Federal Bureau of Investigation

Subscribed and sworn to before
me this 13th day of January 2019,
in Providence, Rhode Island



PATRICIA A. SULLIVAN
United States Magistrate

EXHIBIT 1

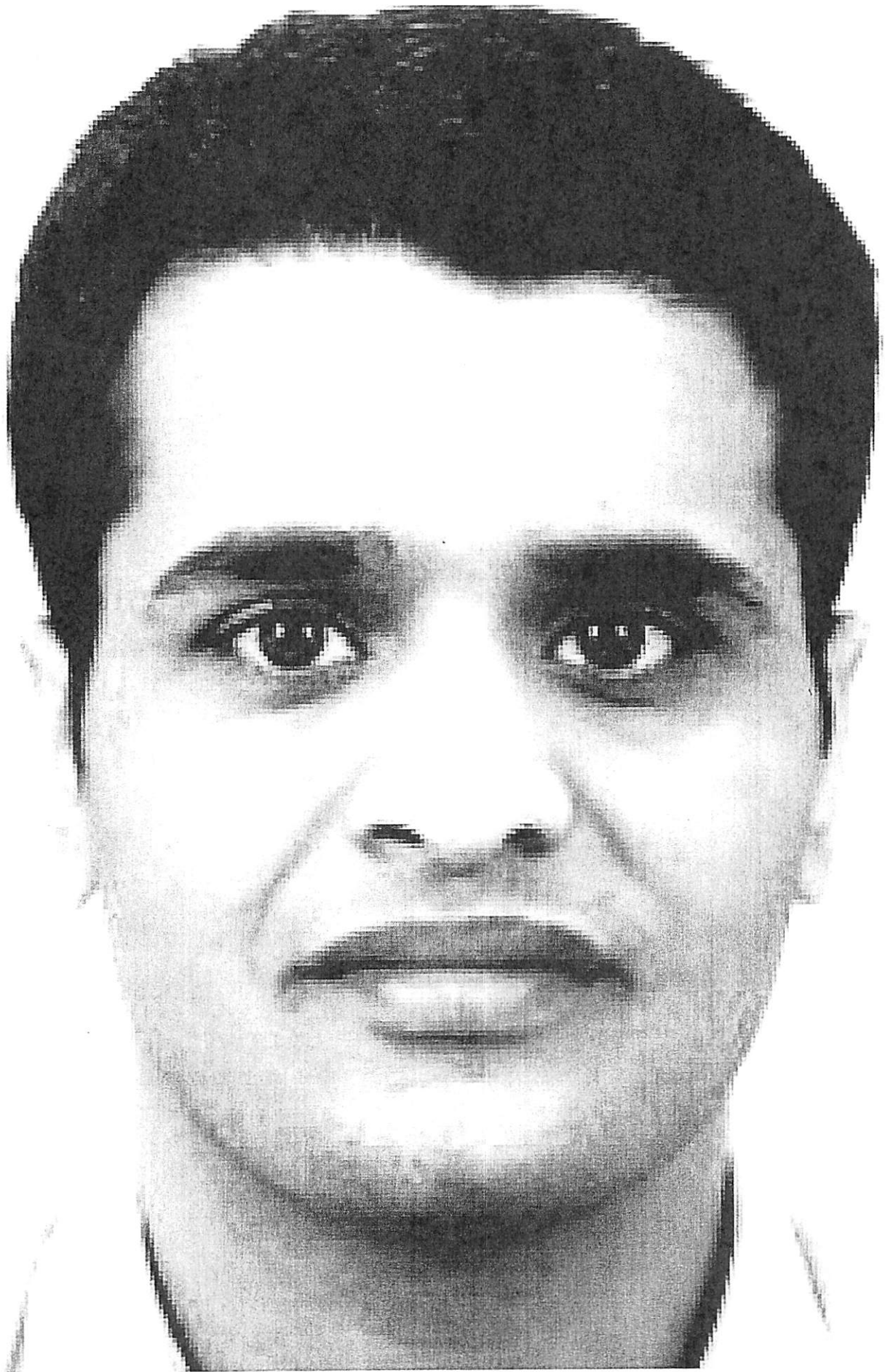


EXHIBIT 2

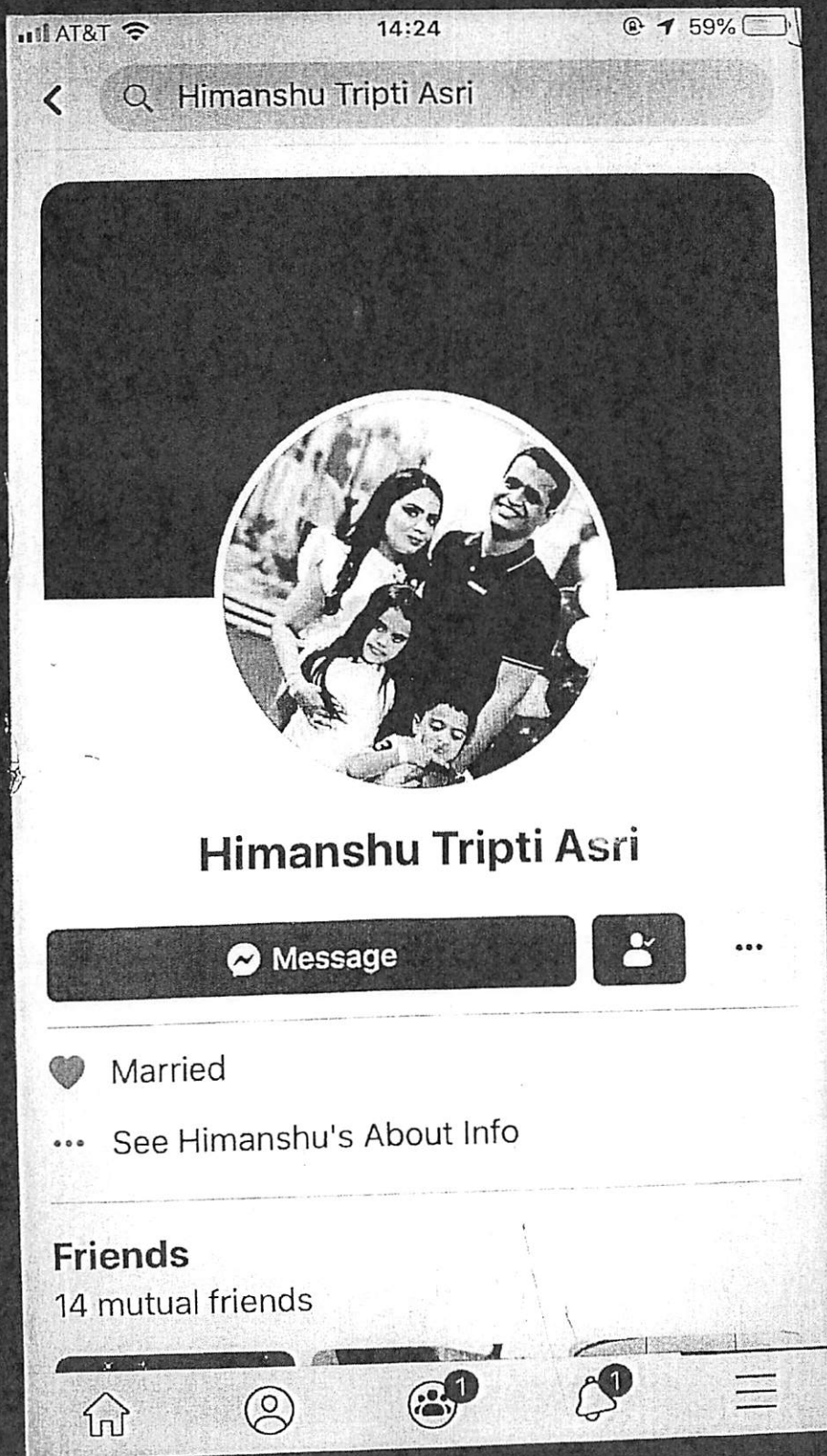


EXHIBIT 3

